CREDENTIAL 104281421

Master Disclosure Record

Document Class:	Federal Disclosure — Unauthorized Credential Persistence
Credential ID:	104281421
Originating System:	RegOnline / Cvent via American Tradeshow Services (ATS)
Filing Party:	Courtney — IT Technician, Contract Role (2017)
Archive Status:	Immutable public record — Archive.org ARK identifier on file
Generated:	June 13, 2026

This document serves as a consolidated master record of disclosures, evidence, personnel, and identified gaps related to the unauthorized persistence of employee credential 104281421 within federal contractor-adjacent event management infrastructure. Each section constitutes a discrete evidentiary exhibit suitable for submission to SEC, CISA, FBI, OIG, or DTCC.

01	**Master Timeline**	Credential discovery through retaliation pattern
02	**ATS Contractual Chain**	Assignment, authorization, hardcoding decision trail
03	**Federal Contractor Exposure Scope**	Jurisdictional reach and affected systems
04	**Response Tracking**	Filing status, receipts, and agency responses

EXHIBIT 01

Master Timeline

Linear chronology from credential assignment through unauthorized persistence, federal disclosure filings, and documented retaliation. Dates represent known anchors; gaps flagged for evidentiary development.

2017 — **Contract Role Initiated** — CONFIRMED

Courtney assigned employee credential ID 104281421 during contract engagement. Credential issued through standard onboarding process.

2017 — **Credential Hardcoded Into ATS Infrastructure** — CONFIRMED — UNAUTHORIZED

Credential 104281421 embedded without authorization into RegOnline/Cvent event management infrastructure operated by American Tradeshow Services (ATS). This action was not disclosed to credential holder.

2017–Present — **Unauthorized Persistence Period** — CONFIRMED

Credential persisted across multiple years in live production systems touching federal contractor-adjacent infrastructure. Duration and full scope of active use undetermined pending system log discovery.

Pre-Disclosure — **Discovery of Unauthorized Hardcoding** — CONFIRMED

Courtney discovers that credential 104281421 has been hardcoded into ATS/RegOnline/Cvent infrastructure without authorization or knowledge of the credential holder.

Filing Period — **SEC TCR #17678 Filed** — FILED

First SEC Tip, Complaint, or Referral submitted. Initiated formal federal disclosure record.

Filing Period — **SEC TCR #17713 Filed** — FILED

Second SEC TCR. Supplemental disclosure.

Filing Period — **SEC TCR #17725 Filed** — FILED

Third SEC TCR. Scope expansion or additional evidentiary submission.

Filing Period — **FBI IC3 Complaint Filed** — FILED

Internet Crime Complaint Center submission documenting unauthorized credential use and infrastructure exposure.

Filing Period — **Six DTCC Cases Filed** — FILED — 6 CASES

Depository Trust and Clearing Corporation filings. Jurisdictional relevance: federal contractor financial infrastructure exposure.

Filing Period **OIG Filing Submitted** **FILED**

Office of Inspector General disclosure. Specific agency OIG to be confirmed in response tracking exhibit.

March 4, 2026 **CISA Incident Report Filed** **FILED — IMMUTABLE RECORD**

CISA Incident Report Form submitted. Simultaneous Archive.org immutable record created with permanent ARK identifier.

March 4, 2026 **Archive.org Permanent Record Created** **ARCHIVED — ARK ID ON FILE**

Public immutable archive of credential case documentation. ARK identifier constitutes permanent timestamped evidentiary anchor.

Post-March 4, 2026 **CISA Vulnerability Disclosure Submitted** **FILED**

Separate CISA Vulnerability Disclosure submission documenting infrastructure exposure specifics.

Post-First SEC Filing **Retaliatory Restraining Order Filed** **DOCUMENTED RETALIATION**

St. Tammany Parish case #2026-10181 filed shortly after first SEC disclosure. Documented as Dodd-Frank Section 21F(h) retaliation pattern. Timing correlation constitutes material retaliation evidence.

Post-Disclosure **Supplemental SEC TCR Filed** **FILED**

Supplemental TCR documenting defective service of restraining order as additional retaliation evidence under Dodd-Frank 21F(h).

TIMELINE GAPS — PRIORITY DEVELOPMENT

- Exact date of unauthorized hardcoding decision — requires ATS internal records
- Specific contract/SOW that governed 2017 engagement — see Exhibit 02
- System log evidence of credential active use across persistence period
- Precise identity of individual(s) who executed hardcoding decision
- Exact dates of all SEC TCR filings (filing period listed; precise dates to be confirmed)
- Federal contractors specifically touched — see Exhibit 03

EXHIBIT 02

ATS Contractual Chain

Documentation of the contractual and personnel chain governing the 2017 engagement, credential assignment, and the unauthorized hardcoding decision. Key personnel identified to date. Authorization gaps flagged.

Key Personnel

Name	Organization	Role / Notes
Keith LeBlanc	ATS	Primary identified figure. Role in credential assignment and/or hardcoding decision to be c
Karen LeBlanc	ATS	Identified ATS personnel. Specific role in credential lifecycle to be documented.
Mike Schwartz	ATS	Identified ATS personnel. Specific role in credential lifecycle to be documented.
Pete Schulz	ATS	Identified ATS personnel. Specific role in credential lifecycle to be documented.
Mike Truesdell	ATS	Identified ATS personnel. Specific role in credential lifecycle to be documented.

Systems Involved

RegOnline

Event registration platform. Credential 104281421 hardcoded into active configuration.

Cvent

Enterprise event management platform. Credential persistence documented across Cvent infrastructure.

American Tradeshow Services (ATS)

Operator entity. Contractual relationship with filing party through 2017 contract role.

CONTRACTUAL CHAIN GAPS — PRIORITY DEVELOPMENT

- Original contract / Statement of Work (SOW) from 2017 engagement — obtain or subpoena
- Documentation of what access 104281421 was authorized to have under that contract
- Any amendment, extension, or renewal that would have governed credential post-contract
- ATS internal change management records for RegOnline/Cvent configuration
- Who specifically executed the hardcoding: technical operator vs. management decision
- Whether ATS disclosed credential use to RegOnline/Cvent platform operators
- Whether RegOnline/Cvent platform operators disclosed to their federal contractor clients

EXHIBIT 03

Federal Contractor Exposure Scope

Jurisdictional weight of the credential case derives from the federal contractor infrastructure connected to RegOnline/Cvent at the time of unauthorized persistence. This exhibit documents the known exposure surface and identifies the evidentiary development needed to establish full scope.

Exposure Surface Analysis

RegOnline and Cvent are enterprise-grade event management platforms used extensively by federal agencies, federal contractors, defense contractors, financial sector entities, and critical infrastructure operators to manage conferences, training events, and government-adjacent gatherings. A hardcoded credential persisting in this infrastructure represents potential unauthorized access to attendee data, organizational data, and event logistics for any entity using these platforms during the persistence period.

Jurisdictional Basis by Filing

Filing	Jurisdictional Basis	Exposure Relevance
SEC TCRs (3 filings)	Securities fraud / market integrity Dodd-Frank whistleblower	Federal contractor data exposure relevant to publicly traded entities
FBI IC3	Federal cybercrime statute 18 U.S.C. § 1030 (CFAA)	Unauthorized computer access across interstate systems
DTCC (6 cases)	Financial market infrastructure clearing system integrity	Federal contractor financial exposure via connected systems
OIG	Inspector General Act Federal program integrity	Contractor misconduct affecting federal programs
CISA Incident Report	CISA critical infrastructure mandates	Event management infrastructure as critical infrastructure vector
CISA Vuln. Disclosure	Coordinated vulnerability disclosure framework	Specific infrastructure vulnerability documentation

Dodd-Frank Retaliation Nexus

The filing of St. Tammany Parish restraining order #2026-10181 shortly after the first SEC TCR submission creates a documented temporal correlation constituting material evidence of Dodd-Frank Section 21F(h) retaliation. Section 21F(h) prohibits retaliation against individuals who provide information to the SEC in good faith. Defective service of the restraining order, documented in the supplemental SEC TCR, further strengthens the retaliation pattern.

EXPOSURE SCOPE GAPS — PRIORITY DEVELOPMENT

- Identify specific named federal contractors that used RegOnline/Cvent during persistence period
- Obtain RegOnline/Cvent client lists for 2017–present timeframe via subpoena or FOIA
- Determine whether any federal agency directly used affected infrastructure
- Quantify number of events and attendee records potentially accessible via hardcoded credential
- Establish whether credential conferred read-only or read-write access to connected records
- Document any evidence of actual access or data exfiltration during persistence period
- Confirm DTCC case jurisdictional basis — which specific financial entities are named

EXHIBIT 04

Response Tracking

Status of all filed disclosures. Acknowledgment receipts, agency responses, case numbers, and follow-up requirements. Gaps indicate missing confirmation documentation that should be obtained and archived.

Filing / Case	Agency / Recipient	Status	Action Required
SEC TCR #17678	SEC — Office of the Whistleblower	**FILED**	Confirmation receipt status unknown — obtain TCR submission confirmation number and archive
SEC TCR #17713	SEC — Office of the Whistleblower	**FILED**	Confirmation receipt status unknown — obtain and archive
SEC TCR #17725	SEC — Office of the Whistleblower	**FILED**	Confirmation receipt status unknown — obtain and archive
Supplemental SEC TCR (Retaliation — Defective Service)	SEC — Office of the Whistleblower	**FILED**	Documents Dodd-Frank 21F(h) retaliation. Confirmation receipt to be archived.
FBI IC3 Complaint	FBI — Internet Crime Complaint Center	**FILED**	IC3 complaints generate a reference number upon submission. Obtain and archive reference number.
DTCC Case 1 of 6	DTCC	**FILED**	Case number and acknowledgment to be documented
DTCC Case 2 of 6	DTCC	**FILED**	Case number and acknowledgment to be documented
DTCC Case 3 of 6	DTCC	**FILED**	Case number and acknowledgment to be documented
DTCC Case 4 of 6	DTCC	**FILED**	Case number and acknowledgment to be documented
DTCC Case 5 of 6	DTCC	**FILED**	Case number and acknowledgment to be documented
DTCC Case 6 of 6	DTCC	**FILED**	Case number and acknowledgment to be documented
OIG Filing	Office of Inspector General (Agency TBD)	**FILED**	Specific OIG agency to be confirmed and documented. Obtain submission reference.
CISA Incident Report March 4, 2026	CISA — Cybersecurity and Infrastructure Security Agency	**FILED — ARCHIVED**	Simultaneous Archive.org record created. ARK identifier on file. CISA acknowledgment receipt to be documented.

CISA Vulnerability Disclosure	CISA — Coordinated Vulnerability Disclosure Program	**FILED**	Submission confirmation and CVD tracking number to be documented.
St. Tammany Parish RO #2026-10181	St. Tammany Parish Court	**DOCUMENTED RETALIATION**	Filed post-SEC disclosure. Documented as Dodd-Frank 21F(h) retaliation. Court records to be fully archived including defective service documentation.

RESPONSE TRACKING GAPS — PRIORITY DEVELOPMENT

- Obtain and archive all SEC TCR submission confirmation numbers (#17678, #17713, #17725, supplemental)
- Obtain and archive FBI IC3 reference number
- Document all six DTCC case numbers individually with dates filed
- Identify which specific OIG office received the OIG filing and obtain reference number
- Obtain CISA Incident Report acknowledgment receipt and document alongside ARK identifier
- Obtain CISA CVD tracking number for Vulnerability Disclosure submission
- Fully archive St. Tammany Parish case #2026-10181 records including defective service proof
- Create a single acknowledgment receipt archive file (PDF or folder) for all filings
- Track any agency substantive responses — none documented to date
- Set calendar follow-up dates for any filings past typical agency response windows

END OF DOCUMENT — Generated June 13, 2026 — Credential 104281421 Master Disclosure Record — All four exhibits constitute permanent evidentiary record.